UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,918	06/29/2001	Brian Jacoby	06975-203001/Security 14	5947

26171 7590 04/29/2009
FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
BOUTAH, ALINA A	
ART UNIT	PAPER NUMBER
2443	

NOTIFICATION DATE	DELIVERY MODE
04/29/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

RECORD OF ORAL HEARING

UNITED STATES PATENT AND TRADEMARK OFFICE

____

BEFORE THE BOARD OF PATENT APPEALS

AND INTERFERENCES

____

EX PARTE BRIAN JACOBY and CHRISTOPHER J. WRIGHT

____

Appeal 2008-4795
Application 09/894,918
Technology Center 2400

____

Oral Hearing Held: March 18, 2009

____

Before HOWARD B. BLANKENSHIP, JAY P. LUCAS, and THU A. DANG, *Administrative Patent Judges.*

APPEARANCES:

ON BEHALF OF THE APPELLANTS:

Chen Qian, Esquire
Tom Rozylowicz, Esquire
FISH & RICHARDSON, P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022

The above-entitled matter came on for oral hearing on Wednesday, March 18, 2009, at The U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia, before Victor Lindsay, Notary Public.

MS. BOBO-ALLEN: Good morning. Calendar No. 22, Appeal No. 2008-4795. Ms. Qian.

MS. QIAN: May it please the court, my name is Chen Qian. I'm from Fish & Richardson. I represent America Online in this application, deep packet scanning.

JUDGE BLANKENSHIP: Little bit -- speak louder, please.

MS. QIAN: Okay. Do I need to review --

UNIDENTIFIED SPEAKER: You can go to the --

MS. QIAN: Oh, okay. Should I repeat? Okay, sorry.

My name is Chen Qian from Fish & Richardson. I represent America Online on the appeal case of deep packet scanning, this application.

America Online, as you know, is a very big internet service provider and provides a lot of web services to many millions of users both nationally and internationally, and they have been doing this for a decade. Of course, they have lots of challenges while being such a big service provider. One of the challenges is they face a lot of attackers. Hackers in the internet community try to inundate servers so that server cannot operate normally in the normal -- for normal users.

So this is area problem and they did a lot of thinking and come up with a lot of solutions. One of them is the application today, deep packet scanning. So in the typical context, AOL will be access provider, which is a server, we claim access provider in the claims, and a client if access request -- request service from the server. So the problem we're trying to do is we want to prevent hackers from attacking the server. So one of the techniques is denial service technique. What they do is they pretend to be a -- user and they log in to the server consecutively so many times in very short duration, so server will be so overwhelmed accepting the hacker's request and then has no bandwidth to process normal users' requests.

To protect the server from such attack, AOL come up with solution that we will introduce a network device sitting between the access requester and access provider. What this network device is doing is it will monitor and try to find attackers and deny them such service. So in detail what it does is in the beginning when access requester requests service, we don't know if it's attack or not so -- we see access provider side. That access provider receives a request. Okay, this is not a legitimate user. I don't have a login password for this guy. Access provider make a decision, this is bad login and provide that feedback back to the access requester buying the -- that request.

So what my device is -- the first function is watching traffic from the server, a person that contacts a network, the traffic unit's data packet. All these communications are data packets. Network service -- network device is watching the data packets from access provider and look to see if there are any login failure messages. The way he does it is to go to -- data packet usually has two portions. One is like -- portion. The other one is the -- portion. -- portion is a contact -- portion is maybe where you'll find where the IP address is, what time you send this packet, all those --

So -- thing about the network device is it goes deep packet scanning going to the -- portion of the packet and check this three different pattern that matches a login failure message. So when you text that, okay, this is -- these are now good. So I'm going to keep -- is this -- requested --

JUDGE LUCAS: Ms. Qian, Ms. Qian, I'm sorry to interrupt you but you have labeled that figure 1, and is that figure 1 on the record in the record?

MS. QIAN: Yes, it is. This shown in the pre-appeal brief -- repeat appeal brief and the answers so --

JUDGE DANG: Right, but it's not in your specification. It's basically -- it was in your arguments in the appeal brief and the brief, yes.

MS. QIAN: Yeah, yes.

JUDGE DANG: Yes, I understand.

MS. QIAN: Yeah.

JUDGE DANG: Oh, yeah, I mean basically we do understand the, the technology. If you want to go through the arguments, we can do that.

MS. QIAN: Yeah, definitely, okay. So you know this -- in between. Look at the -- count in the palo (phonetic sp.) portion -- count the number of attacks. When it's over it's -- value of packets I counted as bad. I will deny subsequent requests from this guy. So that's monitor, deny, two action in this device. That's what we are claiming.

So -- has Examiner provide full references in combination to reject this application so -- reference is a Cox reference. What Cox reference does, it does has -- provider and has intermediate network device. What it does is it's almost like a future, future any bad request from the access provider, because it already has knowledge who might be bad. So what it does is it checks the data package from the access requester, find the IP address of that access requester, and if it, if it knows that this IP address is from attacker I will deny it. Because he has knowledge what kind of IP address is actually fake or from hackers.

So all this guys does is look at data packets from access requester and look at the attribute portion and deny the known attackers.

JUDGE DANG: But if you look at figure 1 of Cox, the arrows go both ways. The -- it goes both ways and so why are -- I mean, you know, you're, you're drawing your number two right there as an -- just, just the data packet going one way. But according to the figure 1 of Cox, the data packets go both ways.

MS. QIAN: The data packet in Cox is going both ways between the client and network device, but they never actually reach to the access provider. The two embodiment they had is once I know it's IP address. The other one is I make some request with access requester and they can acknowledge it. If there's nothing written acknowledge back, I know it's not actually someone who's waiting. It's just computer so I know.

So in those two embodiments, even though it does do little back and forths, okay, request me and then if you don’t acknowledge me, here, I will deny you again. So in those cases, everything is done at network device level, never actually pass -- to the provider service.

MR. ROZYLOWICZ: And to amplify one thing that she said, it never actually makes a decision of whether or not to block this guy based on the response from the access provider to the access requester as it's seen by the network device. It never makes this blocking decision based on that traffic flow right there.

MS. QIAN: -- intelligence is Cox is -- network service. They never actually receive -- access provider to do some login checking and then deny it and based on service decision to accumulate that knowledge. So network device is almost like a future -- I don't even let him reach the server.

JUDGE DANG: Okay. Another question I have is what in your claim, what -- claim 1. What, what in your claim 1 said -- would say that access requester is the I guess attacker of Cox in figure 1 and what would, what would be the access provider that -- I mean you're reading the access provider as the corporate private network, right? But what in your claim particularly defines these terms?

MS. QIAN: Well, it's common sense when you request --

JUDGE DANG: All we have is, all we have is a label that says access requester and access provider.

MS. QIAN: Right.

JUDGE DANG: So you go there -- you go to Cox, and you say okay, I'm going to label it like this, and I'm going to have this figure 2, and I'm going to call this access requester, this access provider. I want to, I guess, hear your, your correlation between Cox and what you would label that. What, what in your claim would say that?

MS. QIAN: Well, so it's kind of based on the language itself. Access requester is by common sense someone try to get service from a server.

JUDGE DANG: Yeah, is -- I mean I, I don't have a -- I don't see a step of accessing service. All you have is access requester. Accessing what?

MS. QIAN: Accesses service.

MR. ROZYLOWICZ: Ms. Qian, do you want to pull up the claim 1, reference that -- it speak to what appears in the claim?

JUDGE LUCAS: While we're waiting, Ms. Qian, would you introduce your associate?

MS. QIAN: Excuse me?

JUDGE LUCAS: Would you introduce your associate?

MS. QIAN: Oh, Tom is my supervisor actually. Tom Rozylowicz.

MR. ROZYLOWICZ: My name is Tom Rozylowicz, Your Honor.

MS. QIAN: From also Fish & Richardson.

Well, the, the claim language in claim 1 said message for securing accessible computer system. So the computer system is the one that's being accessed. The system --

JUDGE DANG: That's in the preamble, right?

MS. QIAN: It's in the preamble, yes, and the, the first -- receiving more than one packet at network device, each packet including palo portion -- portion -- between these, one access requester and at least one access provider through the network device.

So it's -- you access computer system and the system is access provider and there is data packs going between.

Second language, monitoring at the network device. At least the palo portion of the data packet directive at least from one of the access providers to at least one of access requesters by scanning the palo portion for at least one predetermined patent and count the number of data packets having palo portions that include predetermined patent. So that kind of a direction of traffic is we're watching data packets directed from access provider back to the access requesters by scanning the palo portion and counting number of the packets have a patent.

The third step, using the network device deny -- to denying communication with subsequent data packets from access requester to the access provider when number of palo portions that the data packets received from access provider to access requester are deemed to be include predetermined patent exceed -- number.

So, so that just describes the network device -- denying access from the access requester after it find that there's -- certain number of data packets that from access provider that contains a bad patent. In fact, the, the Examiner's answer actually admitted that Cox doesn't teach the access -- the traffic from access provider to the access -- to the network device.

JUDGE DANG: Okay, that's -- let's go on, let's go on to your other arguments.

MS. QIAN: Okay. So just to, to see what deficiencies that Cox has. Cox has quite a few number of deficiencies. Number one it doesn't -- this minor deficiencies like it doesn't show to deep packet scanning, only do the palo portion, and Examiner brings the Maher to cure that deficiency. The other one is Cox didn't really count number of bad packets from -- and what the most significant we think, the whole structure, the whole flow is missing is Cox never look at traffic from access provider. It only -- it did some preemptive strike instead of doing anything based on the intelligence of the server. So to, to cure that deficiency, the Examiner brought Alcendor to cure this deficiency which really doesn't, doesn't help. We'll, we'll take a look at what Alcendor's pointing.

So Alcendor is a telephone system. It's not -- telephone system that used to access -- configure certain services and the, the patent is focused on -- authentication because they think use the ID password or PIN. It's so easy to intercept it by -- they don't trust -- they use telephone, use voice authentication. And what it does is this is speaker of the telephone. Calls to the service provider, say okay, I want configure my internet service. I want configure my TV service. For example, the, the -- shows is like internet service I want control the violence level because I'm -- my child will see violence content. Or it's a TV service. I want to see pay-per-view. I will configure those thing.

So the, the authenticated parent calls the service, say okay, I want to change my minor's level of internet service, and the service provider has a sample of the parent's voice, so he can okay, you are, you are the real parent. Then I will let you configure our service, and if it's a child who is trying to pretend to be a parent and want to see some interesting things, so he calls and he will fail.

So what happens when failed login happens? So when the child calls, say okay, I want to configure my internet service and as -- no, you are not the right -- you are not right subscriber. I will redirect you to the starter page. The start page is whether you want to configure TV service, whether you configure your internet service.

So the child going to try again. So okay, fine. I'm going to call again. I'm going to use a different voice. So this is a very old-fashioned way -- some access provider or the server to say -- to identify whether there is valid login and how the server decides whether it's valid or not, the decision is to redirect to a different page.

So, so Cox and Alcendor even if they combine, we don't see any traffic coming from access provider back to the access provider, because the decision is consumed by an access provider itself and redirect start page -- server flow. So number two, it never showed an adequate device, so --

JUDGE DANG: But the rejection is based on four references, not just two references.

MS. QIAN: Yes.

JUDGE DANG: And the test for obviousness is what the combination of all the references will have --

MS. QIAN: Right.

JUDGE DANG: -- just suggested. Now what about the other references? What about Maher for instance?

MS. QIAN: Yeah --

JUDGE DANG: Maher shows that you are looking at the payload of the --

MS. QIAN: Exactly.

JUDGE DANG: -- of the provider on --

MS. QIAN: No --

JUDGE DANG: -- or if you would label it, you would label it "provider."

MS. QIAN: No, no, actually Maher is looking at the access requester. Both Maher and the --

JUDGE DANG: Maher is looking at packets from the network which is I guess would be "provider."

MS. QIAN: No, actually if you read it deeper the -- from network is from the client.

MR. ROZYLOWICZ: It's network packets from the client side.

MS. QIAN: Yeah.

MR. ROZYLOWICZ: To the access provider.

MS. QIAN: Yeah, data packet can go either way so --

JUDGE DANG: Exactly, and that's what I've been saying. Data packets could go either way.

MS. QIAN: Right.

JUDGE DANG: And so -- but this one says we scan -- I guess they're doing it for -- traffic flow, and traffic flow would be coming from the network and, and you know, I guess it's providing data, it's providing data. Why wouldn't it be an access provider? I don't -- you know, I guess I'm still --

MS. QIAN: Yeah, I guess you --

JUDGE DANG: I'm still not seeing that from your claim as in what is an access requester? What is an access provider?

MS. QIAN: Yeah, I think probably we kind of think it's a system, computer system, so the provider mostly are service providers, and then when user are requesters, and most of the -- are kind of blocking traffic from, from client, because only client can be evil. They can be hackers. Server usually don't --

MR. ROZYLOWICZ: Your Honor, if I paraphrase your question, make sure I'm being responsive because I know we haven't been -- I don't think we've been responsive to it today, and I think if I understand what you're getting at correctly is what is the language in the claim itself that allows us to, to construe claim 1 so that it, it looks like this architecture as opposed to the Cox and other architectures? How do we get the meaning because the, the language in the claim itself only speaks to data packets, not necessarily requests and responses to the requests and I think --

JUDGE DANG: Right. I mean, basically what we -- I'm seeing is receiving from one to another and monitoring it and then, and then denying, right? So there's no step of accessing or, or providing any services or anything like that. So I just need to -- a little clarification as to why one of ordinary skill in the art with access to all four of these references would say hey, that's not obvious.

MR. ROZYLOWICZ: So there's two questions. There --

(Buzzer sounds)

MR. ROZYLOWICZ: Okay, is that 1 minute? Okay, so the first point is that I think we -- for construction we simply attach a lot of meaning to the terms access requester, access provider. That's how we get the -- the other point as to why it’s not obvious to compile these references, this reference right here, Alcendor, simply doesn't protect the server's system from having to respond to the excess number of requests. It simply doesn't protect it. Similarly, Cox there relies upon -- simply operates differently, because it relies on having an established blacklist of who the bad guys are. None of those are directed to a world in which you don't know who your good and bad guys are, and you have to make that decision in real time using a network device that --

JUDGE DANG: Wait, wait. Cox doesn't say who's the bad guy? I thought Cox -- that's what attacker is -- a bad guy, right?

MR. ROZYLOWICZ: Yes, Your Honor.

MS. QIAN: Cox knows, Cox knows who the bad guy is but we don't know --

JUDGE DANG: Right, right, so, so I'm, yeah, I'm, I'm hearing arguments that this one doesn't disclose this. This one doesn't disclose this. I just want to hear an explanation why all of them combined would not be obvious or, you know, would be -- would not have suggested that to one of ordinary skill in the art.

MS. QIAN: Your Honor, I would just say Maher and Eichstaedt and Cox Street (phonetic sp.) all look at the, the incoming traffic. The only one who actually did some login, that's why the print Alcendor and -- we don't -- even with Street we don't have that feature of looking at the server, so that's why we'll bring Alcendor. Alcendor is only because the server decide the login failure. They think that's kind of similar. But the only thing the server did decide login -- that message not returned to the network device to, to -- for determination of -- for the log. So this one has never -- Alcendor is never logged on the server side. So it's like the Street patent, three combinations still fail this -- missing this feature and uses fourth one. The fourth one really didn't do the job. That's why -- it's not --

JUDGE BLANKENSHIP: Would you like a minute to sum up?

MS. QIAN: Sure. So in conclusion, we conclude that even with the four combinations, they still different from what the applicant has claimed. They're missing the significant feature of watching traffic on the server and to make a decision based on the server --

JUDGE BLANKENSHIP: All right, thank you.

MS. QIAN: Thank you.

MR. ROZYLOWICZ: Thank you, Your Honor.

(Whereupon, the proceedings concluded on March 18, 2009.)